CSA Certificate of Cloud Security Knowledge (CCSK)

CSA CCSK

Course Length: 3 Days

Class Code: CT-CCSK1

Overview:

The CCSK training program is a cloud security knowledge and development course focusing on a wide range of foundational cloud security topics. Students attending this course will learn about cloud computing and the security aspects needed to be addressed prior to deployment of any system in a public or private cloud.

Much like the certification exam, this course provides students with a heavy dosage of the CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3 and the ENISA report Cloud Computing: Benefits, Risks and Recommendations for Information Security.

Course Objectives:

Principles of Privacy Program Management is the how-to training on implementing a privacy program framework, managing the privacy program operational lifecycle and structuring a knowledgeable, high-performing privacy team. Those taking this course will learn the skills to manage privacy in an organization through process and technology—regardless of jurisdiction or industry.

The Principles of Privacy Program Management training is based on the body of knowledge for the IAPP's ANSI accredited Certified Information Privacy Manager (CIPM) certification program.

Target Student:

The intended audience for CCSK training is people interested in learning more about cloud computing and security, along with IT professionals interested in obtaining the Certificate of Cloud Security Knowledge (CCSK).

- Professionals interested in obtaining the CCSK credential
- IT Security Professionals
- IT Auditors
- Managers, Directors and Executives
- System Architects
- Compliance Specialists
- Risk Specialists
- Business Analysts
- Business Unit Stakeholders

Pre-requisites: None

Course Content

Module 1 Introduction and Cloud Architectures

- Define cloud computing
- Cloud computing stack components
- Cloud reference model and security

Module 2 Infrastructure Security for Cloud Computing

- Understand the components of cloud infrastructure
- Assess the security implications of different deployment models
- Advantages and disadvantages of virtual infrastructure
- The cloud management plane
- Different service models security basics

Module 3 Managing Cloud Computing Security and Risk

- Risk and Governance
- Legal and Compliance
- Audit
- Portability and Interoperability
- Incident Response

Module 4 Data Security for Cloud Computing

- Understand different cloud storage models
- Define security issues for data in the cloud
- Introduce data security lifecycle
- Address cloud security and governance
- Apply lifecycle to use cases
- Discuss data encryption

Module 5 Securing Cloud Applications and Users

- Define Application Architecture, Design, and Operations lifecycle
- Discuss impact on SDLC
- Examine Application Security tools and Vulnerability Management
- Discuss role of Compliance in Cloud applications

Module 6 Selecting Cloud Services

- Enabling the security strategy
- Selecting a cloud provider
- Security as a Service (SECaaS)
- Summary and Review

CierraTEC
training@cierratec.net
www.cierratec.net
(678) 389-4322